(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
31. Mai 2001 (31.05.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/39134 A2

(51) Internationale Patentklassifikation[7]: G07C 9/00

(21) Internationales Aktenzeichen: PCT/DE00/04140

(22) Internationales Anmeldedatum:
23. November 2000 (23.11.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
99123206.7 25. November 1999 (25.11.1999) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Strasse 53, 81541 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: HIEROLD, Christofer [DE/DE]; Dornröschenstrasse 48, D-81739 München (DE). LEHMANN, Volker [DE/DE]; Geyerspergerstrasse 53, 80689 München (DE).

(74) Anwalt: EPPING HERMANN & FISCHER GBR; Postfach 12 10 26, 80034 München (DE).

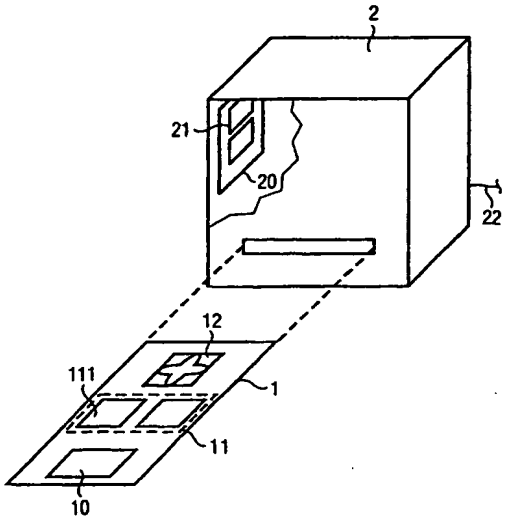
(81) Bestimmungsstaaten *(national)*: BR, CN, IN, JP, KR, MX, RU, UA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: SECURITY SYSTEM COMPRISING A BIOMETRIC SENSOR

(54) Bezeichnung: SICHERHEITSSYSTEM MIT BIOMETRISCHEM SENSOR



(57) Abstract: The invention relates to a security system that uses chip cards (1) comprising a biometric sensor (10), a fingerprint sensor for instance. Biometric information, i.e. the location of fingerprint minutias for instance, that is detected by the sensor (10) is compared to stored reference data which are separated into a first and a second part, whereby said parts are only stored in the data carrier (1) or are only stored in the reading device (2). Data security against the unauthorised reading out of reference information and the security against influencing the current authentication process are thus increased.

(57) Zusammenfassung: Ein Sicherheitssystem verwendet Chipkarten (1) mit einem biometrischen Sensor (10), z.B. Fingerprint-Sensor. Vom Sensor (10) ermittelte biometrische Information, z.B. Ortslage von Minutien des Fingerprints, wird mit gespeicherten Referenzdaten verglichen. Die Referenzdaten sind in einen ersten und einen zweiten Teil aufgeteilt, die nur im Datenträger (1) beziehungsweise nur im Lesegerät (2) gespeichert sind. Dadurch wird die Datensicherheit gegenüber unberechtigtem Auslesen der Referenzinformation sowie die Sicherheit der Beeinflussung des laufenden Authentizierungsvorgangs erhöht.

WO 01/39134 A2

Veröffentlicht:

— *Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Sicherheitssystem mit biometrischem Sensor

Die Erfindung betrifft ein Sicherheitssystem, das umfaßt: eine zentrale Einheit mit einem biometrischen Sensor zur Ermittlung von biometrischen Daten, welche charakteristische biometrische Merkmale einer Person repräsentieren; mindestens einen mobilen Datenträger; ein Speichermittel, um biometrische Referenzdaten, die biometrische Referenzmerkmale für die Person repräsentieren, im System zu speichern; eine Steuerungseinrichtung, um in Abhängigkeit von einem Vergleich zwischen den durch den Sensor ermittelten biometrischen Daten und den Referenzdaten ein Freigabesignal zur Steuerung einer Funktionseinheit erzeugbar ist.

Die Erfindung betrifft außerdem ein Verfahren zum Betrieb eines solchen Sicherheitssystems.

Herkömmliche Sicherheitssysteme umfassen einen Datenträger, beispielsweise in Form und Größe einer Scheckkarte, der einen Sensor enthält, welcher biometrische Charakteristika der Bedienperson ermittelt, um zu gewährleisten, daß die Bedienperson berechtigt ist, den Datenträger zu verwenden. Der Datenträger ermöglicht, in Sicherheitssystemen die Freigabe für den Zugriff auf eine Funktionseinheit. Beispielsweise enthält der Datenträger für Bankanwendungen einen Fingerprint-Sensor und tauscht mit einem Bankautomaten Daten aus, um dem Bediener einen Zugriff auf sein persönliches Konto freizuschalten.

Ein Datenträger mit einem Fingerprint-Sensor ist in der US-Patentschrift 4,582,985 beschrieben. Nachdem die Bedienperson den Finger auf den Sensor aufgelegt hat, wird der Fingerabdruck vermessen, um ein entsprechenden Datenbitstrom zu erzeugen. Dieser wird mit auf der Chipkarte gespeicherter Referenzinformation verglichen. Bei ausreichender Übereinstimmung wird der Datenträger freigegeben, indem ein Signalpfad zwi-

schen Datenträger und Lesegerät freigeschaltet wird. Die Authentizität des Benutzers wird vollständig innerhalb der Chipkarte festgestellt und dem Lesegerät entsprechend mitgeteilt.

Nachteilig ist, daß das Freigabesignal nicht ausreichend geschützt ist. Es könnte bei einem betrügerischen Angriff verfälscht werden, so daß ein nicht authentizierter Benutzer sich trotzdem Zugang zum durch das Sicherheitssystem geschützten Gerät verschaffen könnte. In anderen bekannten Systemen werden daher Freigabesignale durch geeignete kryptologische Verfahren ihrerseits wieder geschützt. Dies erfordert jedoch entsprechenden Schaltungsaufwand für einen Kryptoprozessor auf dem Datenträger und entsprechende Decodiereinrichtungen im Lesegerät. Außerdem könnte im Laufe der Zeit aufgrund der sich weiter entwickelnden Technik der Kryptocode entschlüsselt werden.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Sicherheitssystem der eingangs beschriebenen Art anzugeben, welches ausreichend sicher ist und vergleichsweise geringen Aufwand erfordert.

Gemäß der Erfindung wird diese Aufgabe durch ein Sicherheitssystem der eingangs genannten Art, welches dadurch gekennzeichnet ist, daß die biometrischen Referenzdaten aus einem ersten und einem zweiten Teil gebildet sind und daß der erste Teil im Datenträger und der zweite Teil in der zentralen Einheit gespeichert sind.

Ein Verfahren zum Betrieb eines Sicherheitssystem gemäß der Erfindung ist in Patentanspruch 10 angegeben.

Beim Sicherheitssystem gemäß der Erfindung sind die Referenzdaten, mit welchen die durch den Sensor ermittelten biometrischen Daten verglichen werden, um die Authentizität des Be-

nutzers zu bestimmen, nicht etwa - wie herkömmlich - vollständig auf dem Datenträger gespeichert, sondern verteilt sowohl auf dem Datenträger als auch im Lesegerät. Nur die Kombination von Datenträger und Lesegerät stellt die vollständige Information bereit, welche zur Authentizierung erforderlich ist. Die Information auf der Karte oder im Lesegerät für sich alleine betrachtet reicht nicht aus, um zu authentizieren. Ein Abhören der jeweiligen Teilinformation genügt nicht, um eine Freischaltung zu bewirken. Wenn die auf dem Datenträger bereits vorverarbeiteten Daten an das Lesegerät übertragen werden, ist keine zusätzliche Verschlüsselung notwendig, um trotzdem ein ausreichendes Maß an Sicherheit bei einem Abhörversuch zu erreichen. Die Weiterverarbeitung der im Lesegerät empfangenen Daten bis zur letztendlichen Freigabe kann mit herkömmlichen Mitteln im Lesegerät effektiv vor unberechtigten Eingriffen geschützt werden. Ein Vorteil der Erfindung liegt darin, daß mit dem gleichen Datenträger bei niedrigeren Sicherheitsanforderungen bereits nach dem ersten im Datenträger ablaufenden Identifikationsschritt die Freigabe ermöglicht werden kann.

Besonders zweckmäßig ist die Erfindung, wenn ein biometrischer Sensor verwendet wird, der die charakteristischen Elemente eines Fingerabdrucks ermittelt, ein sogenannter Fingerprint-Sensor. Ein Fingerprint-Sensor bestimmt die ortsaufgelöste Lage von Minutien des Fingerabdrucks. Bei Minutien handelt es sich um singuläre Stellen der Papillarlinien eines Fingerabdrucks. Dies können Endpunkte, Verzweigungen oder ähnliche Stellen der Papillarlinien des Fingerabdrucks sein. Die Ortslage wird als Entfernung zu einem Referenzpunkt, sogenannter Radius, und Winkel zu einer Referenzrichtung bestimmt. Zur Personalisierung des Datenträgers wird vorab der Fingerabdruck des Inhabers des Datenträgers aufgenommen, daraus werden entsprechende Referenzwerte für Radius und Winkel ermittelt und im System gespeichert. Zweckmäßigerweise werden die Radiusreferenzdaten nur auf dem Datenträger gespeichert, die Winkelreferenzdaten werden nur im Lesegerät gespeichert.

Alternativ können die Datenteile in umgekehrter Anordnung gespeichert werden, d.h. die Winkelreferenzdaten im Datenträger, die Entfernungsreferenzdaten im Lesegerät. Die Ausführung der Erfindung ist auch in Zusammenhang mit einem Sensor, der andere biometrische Merkmale der Bedienperson auswertet, denkbar. Beispielsweise könnte sich ein Sensor eignen, der die Struktur der Iris des Auges des Bedieners ermittelt.

Zweckmäßigerweise genügt es, die Messfläche des Sensors in konzentrische, auf einen Referenzpunkt bezogene Ringe oder Segmente aufzuteilen und festzustellen, wie viele Minutien innerhalb eines Radiussegments liegen. Die ermittelte Anzahl der Minutien innerhalb der verschiedenen Radiussegmente wird mit entsprechenden Referenzdaten verglichen. Dieser erste Identifikationsschritt ist erfüllt, wenn eine hinreichende Übereinstimmung zwischen Messung und Referenz vorliegt. In der Praxis haben sich acht konzentrische Entfernungssegmente innerhalb der Messfläche des Fingerprint-Sensors als geeignet erwiesen.

Betreffend die Winkelinformation ist die Messfläche des Fingerprint-Sensors in Winkelsektoren oder -segmente aufgeteilt. Der Fingerprint-Sensor ermittelt, wie viele Minutien innerhalb eines jeweiligen der Segmente liegen. Die Anzahl der für jedes Winkelsegment erhaltenen Minutien wird mit den gespeicherten Referenzwerten verglichen. Bei hinreichender Übereinstimmung zwischen Messung und Referenzwert wird auch der zweite Identifikationsschritt als erfüllt angesehen. Daraufhin erfolgt die Freigabe einer vom Sicherheitssystem überwachten Funktionseinheit. Bei geringerem Sicherheitsbedürfnis wird die Freigabe bereits nach dem ersten Identifikationsschritt geschaltet.

Nachfolgend wird die Erfindung anhand der in der Zeichnung dargestellten Figuren näher erläutert. Es zeigen:

Figur 1 eine Gesamtansicht eines Sicherheitssystems mit Chipkarte und Lesegerät,

Figur 2 ein Beispiel für die Lage der Minutien eines Fingerabdrucks und deren Zuordnung zu Radiussegmenten und Winkelsektoren sowie die in die Auswertung eingehende Radius- bzw. Winkelinformation und

Figur 3 eine Flußdiagramm für den Betrieb des Sicherheitssystems.

Das in Figur 1 dargestellte Sicherheitssystem umfaßt als Datenträger eine Chipkarte 1 und als zentrale Einheit ein Lesegerät 2. Die Chipkarte 1 enthält einen Fingerprint-Sensor 10, auf den der Benutzer einen vorbestimmten Finger liegt und der auf kapazitive Weise den Verlauf der Papillarlinien der Haut vermißt. Die Kommunikation mit dem Lesegerät 2 wird über mechanische Kontakte 12 abgewickelt. Alternativ können kontaktlose, auf elektromechanische Kopplung beruhende Verfahren angewandt werden.

Die vom Fingerprint-Sensor 10 ermittelten Daten werden in einen Mikrokontroller 11 eingespeist, der daraus nach hinreichend bekannten Algorithmen die Lage der Minutien berechnet. Zur Authentizierung wird die örtliche Lage der Minutien mit entsprechenden im System gespeicherten Referenzwerten verglichen. Ein erster Teil der Referenzwerte ist in einem nichtflüchtigen Speicher 111 auf dem Datenträger 1 gespeichert. Zweckmäßigerweise ist der Speicher 111 ein im Mikrokontroller 11 angeordneter ROM-Speicher. Der Mikrokontroller 11 vergleicht einen Teil der vom Fingerprint-Sensor 10 erhaltenen Daten mit den vom Speicher 111 bereitgestellten Referenzdaten.

Wenn der im Datenträger 1 ablaufende erste Identifikationsschritt erfolgreich war, schließt sich nach dem Einschieben des Datenträgers 1 in das Lesegerät 2 ein zweiter Identifikationsschritt an. Die hierzu erforderlichen vom Fingerprint-Sensor 10 gemessenen und vom Mikrokontroller 11 aufbereiteten

Daten werden über die Kontakte 12 in das Lesegerät 2 übertragen und dort an einen Mikrokontroller 20 weitergeleitet. Der Mikrokontroller 20 enthält einen Speicher 21, welcher einen zweiten Teil der Referenzdaten speichert. Nach erfolgreichem Abschluß des im Mikrokontroller 20 ablaufenden zweiten Identifikationsschritts wird ein entsprechendes Freigabesignal an Leitung 22 erzeugt, durch welches eine an das Lesegerät 2 angeschlossene Funktionseinheit freigeschaltet wird. Das Lesegerät 2 ist beispielsweise in einem Bankautomaten enthalten. Nach erfolgreicher Authentizierung des Benutzers wird der Bankautomat freigegeben, so daß Geld abgehoben werden kann oder eine Überweisung oder ähnliche sicherheitsrelevante Aktionen ausgeführt werden können.

Eine zweckmäßige Ausgestaltung des Betriebs des Fingerprint-Sensors 10 wird in Zusammenhang mit Figur 2 an einem beispielhaften Fingerabdruck erläutert. Die eingezeichnete Punkte sind die nach Verarbeitung der Signale des Fingerprint-Sensors berechneten Orte der Minutien des Fingerabdrucks. Durch die Lage der Minutien ist ein Fingerabdruck hinreichend exakt identifizierbar. Die linke Darstellung der Aufsicht auf den Fingerprint-Sensor 10 zeigt acht konzentrische Entfernungs- oder Radiussegmente. Der Mikrokontroller 11 ermittelt die Anzahl der festgestellten Minutien innerhalb eines jeden Segments. Das Ringsegment Nr. 1 enthält drei Minutien 101, 102, 103. Das Ringsegment Nr. 2 enthält zwei Minutien 104, 105 etc. Die vom Mikrokontroller 11 ermittelte Entfernungsinformation beträgt insgesamt 32302200. Diese wird mit einem entsprechenden, bei Personalisierung der Chipkarte 11 im ROM 111 abgelegten Datensatz verglichen.

Bei erfolgreichem Abschluß dieses ersten Identifikationsschritts wird die Winkelinformation an das Lesegerät 2 übertragen und dort weiterverarbeitet. Die Fläche des Fingerprint-Sensors 10 ist in acht gleich große Sektorensegmente aufgeteilt. Der Mikrokontroller 11 ermittelt die jeweilige Anzahl von Minutien, die in jedem der acht Segmente liegt.

Beispielsweise enthält das Segment 1 zwei Minutien 106, 107. Im Segment 2 liegt eine Minutie 108 etc. Die über die Kontakte 12 an das Lesegerät 2 übertragene Winkelinformation umfaßt den Datensatz 21213021. Diese Daten werden im Mikrokontroller 20 mit dem bei der Personalisierung der Chipkarte 1 ermittelten und zentral in dessen Speicher 21 abgelegten Datensatz verglichen. Bei hinreichender Übereinstimmung wird der zweite Identifikationsschritt und somit der gesamte Authentisierungsvorgang als erfolgreich abgeschlossen angesehen.

Wesentlich ist, daß die Radiusreferenzdaten nur auf der Chipkarte 1 und die Winkelreferenzdaten nur im Lesegerät 2 gespeichert sind. Weder auf der Karte, noch im Lesegerät ist die vollständige Referenzinformation vorhanden. Sollte bei einem betrügerischen Angriff versucht werden, die Referenzinformation aus der Karte auszulesen, ist sie alleine wertlos. Die vollständigen Referenzdaten sind an keiner Stelle zusammenhängend abgespeichert.

Der Verfahrensablauf bei der Feststellung der Authentizität des Inhabers einer Chipkarte gegenüber einem Lesegerät ist in Figur 3 insgesamt dargestellt. In einem Schritt 31 liegt eine Karte mit der Radiusinformation 32302200 vor. In einem Schritt 32 stellt die Karte fest, daß der Bediener den Finger auf das Sensorfeld 10 aufgelegt hat. Der Fingerprint-Sensor 10 ermittelt in einem Schritt 33 den Verlauf der Papillarlinien des Fingerabdrucks, woraus der Mikrokontroller 10 die Ortslage der Minutien berechnet und davon die Radius- und Winkelinformation entsprechend dem anhand vom Figur 2 erläuterten Format ableitet. In einem Schritt 34 vergleicht der Mikrokontroller 11 diese durch die Messung erhaltenen Radiusdaten mit den auf der Karte im ROM 111 gespeicherten Daten. Liegt keine Übereinstimmung vor, wird das Identifizierungsverfahren im Schritt 35 abgebrochen. Bei erkannter Übereinstimmung sendet in einem Schritt 36 die Chipkarte die anhand des Fingerprint-Sensors 10 ermittelte Winkelinformation 21213021 an den Mikrokontroller 20 des Lesegeräts 2. Diese

wird dort mit den gespeicherten Winkelreferenzdaten in einem Schritt 37 verglichen. Wenn im Schritt 37 keine Übereinstimmung festgestellt wird, bricht das Lesegerät den Vorgang ab (Schritt 38). Sofern das Lesegerät 2 im Schritt 37 hinreichende Übereinstimmung der ermittelten und gespeicherten Winkeldaten feststellt, wird in einem Schritt 39 ein Freigabesignal an Leitung 22 erzeugt. Das durch das Sicherheitssystem geschützte Verarbeitungsgerät wird dadurch für den Benutzer freigeschaltet. Die von der Chipkarte ermittelte Winkelinformation ist im Mikrokontroller 11 der Karte 1 nur flüchtig gespeichert. Wenn die vom Lesegerät 2 den Datenträger 1 zur Führung gestellte Versorgungsspannung abgeschaltet wird, verliert die Karte diese Winkelinformation nach einigen wenigen Sekunden (Schritt 40).

Vorteilhaft ist, daß bei geringeren Sicherheitsanforderungen bereits nach dem Schritt 35 die Freigabe durch das Lesegerät erfolgen kann. Eine Übertragung der Winkeldaten an das Lesegerät ist dann nicht mehr notwendig.

Patentansprüche

1. Sicherheitssystem, das umfaßt:
- eine zentrale Einheit (2) mit einem biometrischen Sensor (10) zur Ermittlung von biometrischen Daten, welche charakteristische biometrische Merkmale einer Person repräsentieren,
- mindestens einen mobilen Datenträger (1),
- ein Speichermittel (111, 21), um biometrische Referenzdaten, die biometrische Referenzmerkmale für die Person repräsentieren, im System zu speichern,
- eine Steuerungseinrichtung (11, 20), um in Abhängigkeit von einem Vergleich zwischen den durch den Sensor (10) ermittelten biometrischen Daten und den Referenzdaten ein Freigabesignal zur Steuerung einer Funktionseinheit erzeugbar ist,

d a d u r c h g e k e n n z e i c h n e t, daß die biometrischen Referenzdaten aus einem ersten und einem zweiten Teil gebildet sind und daß der erste Teil im Datenträger (1) und der zweite Teil in der zentralen Einheit (2) gespeichert sind.

2. Sicherheitssytem nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t, daß der biometrische Sensor (10) ausgebildet ist, um charakteristische Elemente des Fingerabdrucks eines Fingers der Person zu ermitteln.

3. Sicherheitssystem nach Anspruch 2,
d a d u r c h g e k e n n z e i c h n e t, daß der biometrische Sensor (10) ausgebildet ist, um als die biometrische Daten die örtliche Lage von Minutien (101, ..., 105, 106, ..., 108) des Fingerabdrucks zu ermitteln.

4. Sicherheitssystem nach Anspruch 3,
d a d u r c h g e k e n n z e i c h n e t, daß
der biometrische Sensor (10) ausgebildet ist, die biometrischen Daten als Entfernung relativ zu einem Referenzmeßpunkt und Winkel relativ zu einer Referenzmeßrichtung zu ermitteln.

5. Sicherheitssystem nach Anspruch 4,
d a d u r c h g e k e n n z e i c h n e t, daß der erste Teil der Referenzdaten Datenwerte umfaßt, die die Entfernung von Minutien (101, ..., 105, 106, ..., 108) der biometrischen Referenzdaten von einem Referenzpunkt repräsentieren, und daß der zweite Teil der Referenzdaten Datenwerte umfaßt, die den Winkel der Minutien (101, ..., 105, 106, ..., 108) der biometrischen Referenzdaten relativ zu einer Referenzrichtung repräsentieren, oder umgekehrt.

6. Sicherheitssystem nach Anspruch 5,
d a d u r c h g e k e n n z e i c h n e t, daß
zur Ermittlung der biometrischen Daten auf einen Referenzpunkt bezogene konzentrische Ringsegmente vorgesehen sind, daß der biometrische Sensor ausgebildet ist, Entfernungsdatenwerte zu ermitteln, die die jeweilige Anzahl der in den Entfernungsabschnitten liegenden Minutien (101, ..., 105) der Person repräsentieren, daß die biometrischen Referenzdaten vorgegebene Entfernungsdatenwerte umfassen, die eine jeweilige Anzahl von in entsprechenden konzentrischen Ringsegmente liegenden Minutien der biometrischen Referenzdaten repräsentieren, und daß die ermittelten Entfernungsdatenwerte mit den vorgegebenen Entfernungsdatenwerten verglichen werden, um das Freigabesignal zu erzeugen.

7. Sicherheitssystem nach Anspruch 5 oder 6,
d a d u r c h g e k e n n z e i c h n e t, daß
zur Ermittlung der biometrischen Daten Winkelsegmente vorgesehen sind, daß der biometrische Sensor ausgebildet ist, Win-

keldatenwerte zu ermitteln, die die jeweiligen Anzahl von in den Winkelsegmente liegenden Minutien (106, ..., 108) der Person repräsentieren, daß die biometrischen Referenzdaten vorgegebene Winkeldatenwerte umfassen, die eine jeweilige Anzahl von in entsprechenden Winkelsegmente liegenden Minutien der biometrischen Referenzdaten repräsentieren, und daß die ermittelten Winkeldatenwerte mit den vorgegebenen Winkeldatenwerten der Referenzdaten verglichen werden, um das Freigabesignal zu erzeugen.

8. Sicherheitssystem nach Anspruch 7,
d a d u r c h g e k e n n z e i c h n e t, daß
die vorgegebenen Entfernungsdatenwerte in einem Speicher (111), der auf dem Datenträger (1) angeordnet ist, nichtflüchtig gespeichert sind und daß der Sensor (10) auf dem Datenträger (11) angeordnet ist.

9. Sicherheitssystem nach Anspruch 8,
d a d u r c h g e k e n n z e i c h n e t, daß
die vorgegebenen Winkeldatenwerte in einem Speicher (21), der in der zentralen Einheit (2) angeordnet ist, gespeichert sind.

10. Verfahren nach einem der Ansprüche 1 bis 9,
d a d u r c h g e k e n n z e i c h n e t, daß
- vom Datenträger die biometrischen Datenwerte ermittelt werden (33),
- ein Teil der ermittelten Datenwerte mit dem ersten, auf dem Datenträger (1) gespeicherten Teil der biometrischen Referenzdaten innerhalb des Datenträgers (1) verglichen wird (34),
- bei erfülltem Vergleich ein anderer Teil der ermittelten Datenwerte an die zentrale Einheit (2) übertragen wird (36),

- der übertragene andere Teil der Datenwerte mit dem in der zentralen Einheit (2) gespeicherten zweiten Teil der biometrischen Referenzdaten verglichen wird (37),
- und bei erfülltem Vergleich das Freigabesignal erzeugt wird (39).

11. Verfahren nach Anspruch 10,
dadurch gekennzeichnet, daß
vom Datenträger (1) die Entfernungsdatenwerte und die Winkeldatenwerte ermittelt werden, daß vom Datenträger (1) die Entfernungsdatenwerte mit den auf dem Datenträger (1) gespeicherten vorgegebenen Entfernungsdatenwerten verglichen werden und bei erfülltem Vergleich die ermittelten Winkeldatenwerte an die zentrale Einheit (2) übertragen werden, daß in der zentralen Einheit (2) die übertragenen Winkeldatenwerte mit den gespeicherten vorgegebenen Winkeldatenwerten verglichen werden, um bei erfülltem Vergleich das Freigabesignal zu erzeugen.

FIG 1

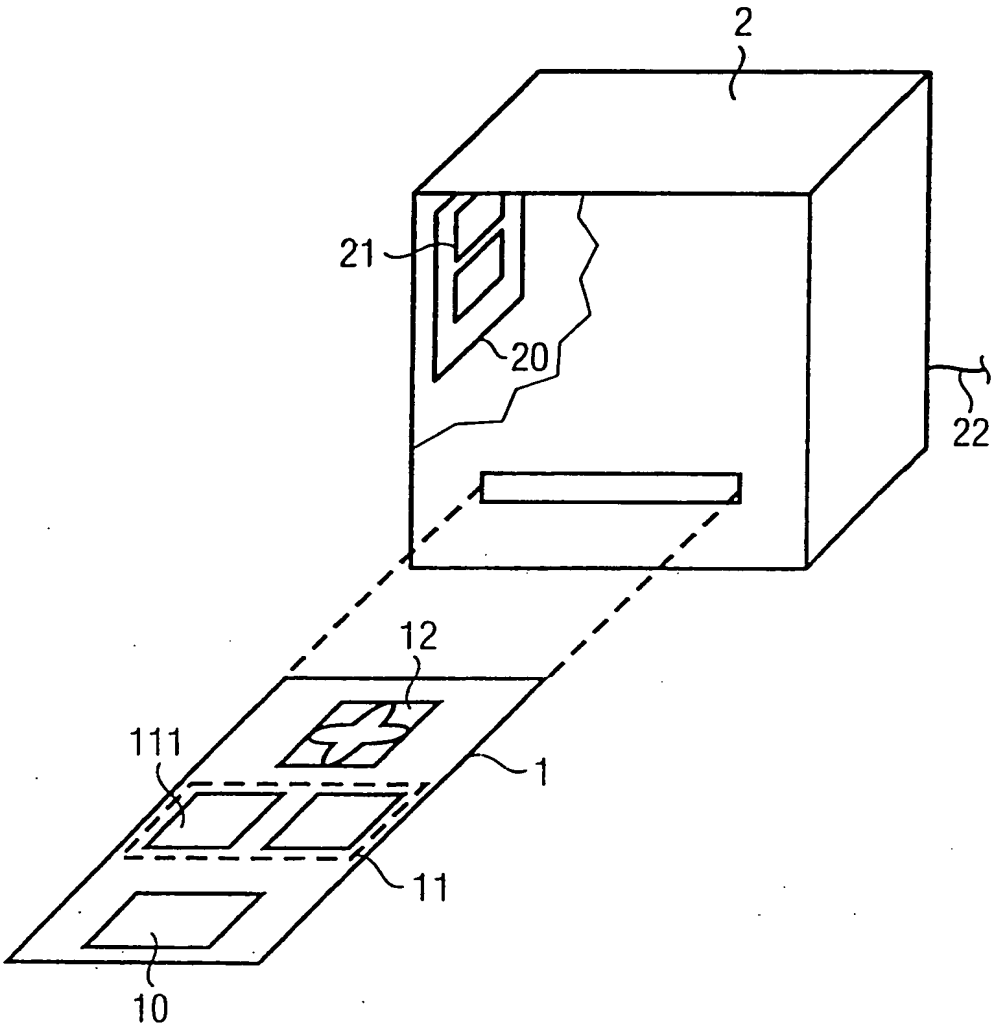


FIG 2

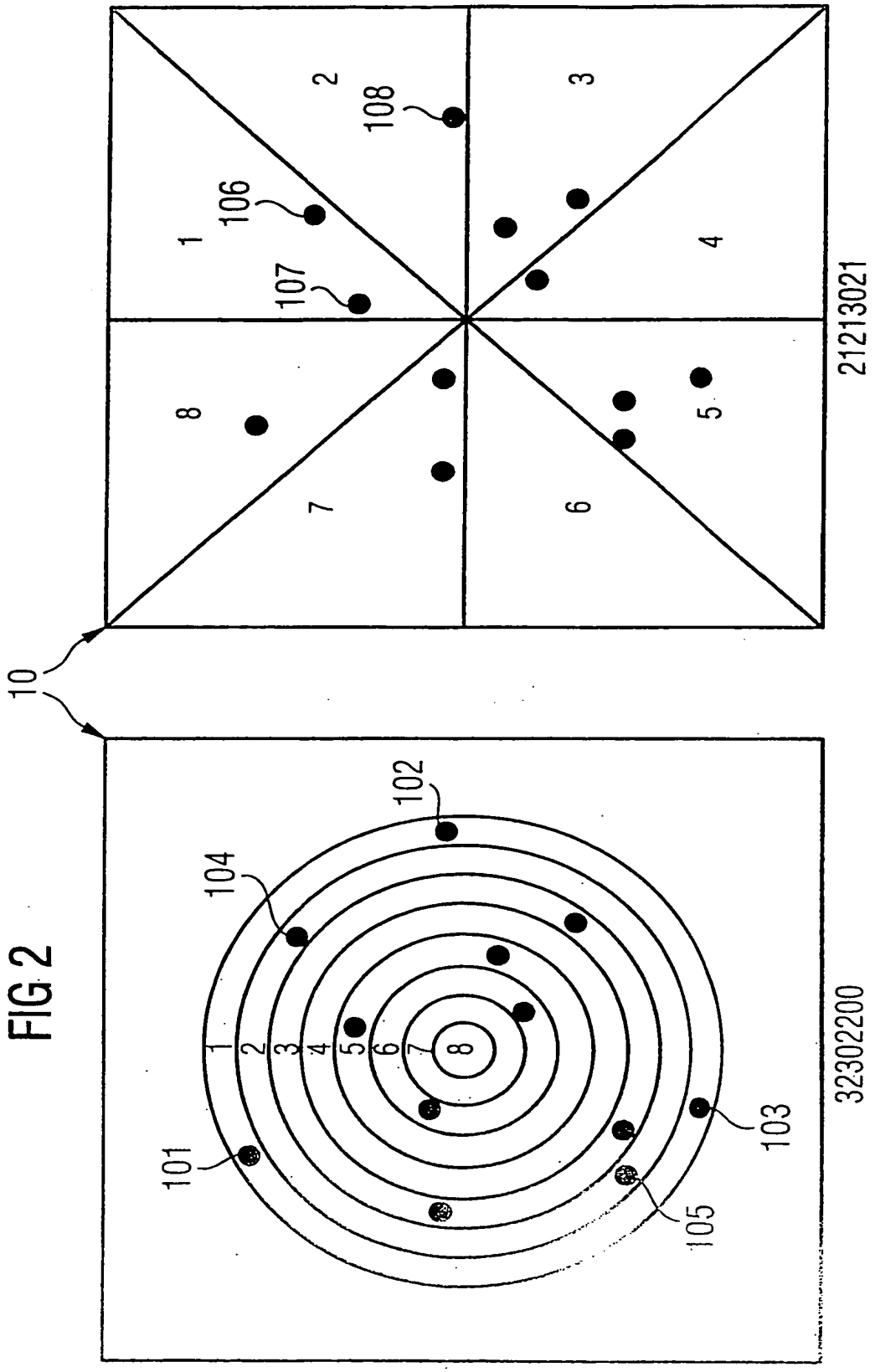
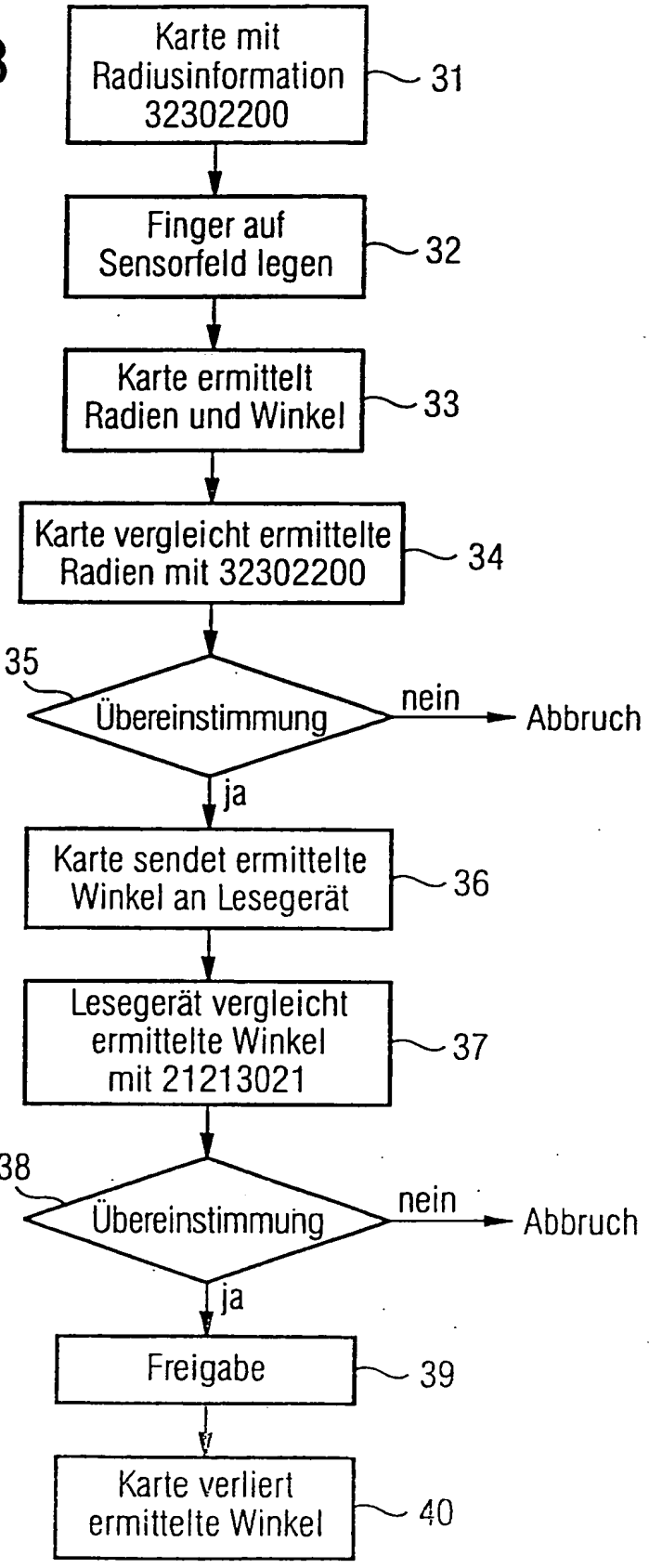

10
1
2
3
4
5
6
7
8
106
107
108
21213021
101
102
103
104
105
32302200

FIG 3


Karte mit Radiusinformation 32302200
31
Finger auf Sensorfeld legen
32
Karte ermittelt Radien und Winkel
33
Karte vergleicht ermittelte Radien mit 32302200
34
35
Übereinstimmung
nein
Abbruch
ja
Karte sendet ermittelte Winkel an Lesegerät
36
Lesegerät vergleicht ermittelte Winkel mit 21213021
37
38
Übereinstimmung
nein
Abbruch
ja
Freigabe
39
Karte verliert ermittelte Winkel
40